AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

For electronic devices : (1) Galaxy Note 8 Cell Phone (2) My Passport Portable Hard Drive (3) LG Cell Phone (4) Samsung Cell Phone all which are more fully described in Attachment A

Case No. 1:19MJ-496

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1962(d)	Conspiracy to Participate in Racketeering Activity

The application is based on these facts:
See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Brian Christ
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/2/19

Judge's signature

City and state: Cincinnati, Ohio

Hon. Karen L. Litkovitz, U.S.M.J.
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF

(1) Galaxy Note 8 Cell Phone
(2) My Passport Portable Hard Drive
(3) LG Cell Phone
(4) Samsung Cell Phone
(5) Large Suitcase Dark Olive Green and Black

CURRENTLY LOCATED AT FEDERAL BUREAU OF INVESTIGATIONS OFFICES AT 2012 RONALD REAGAN DRIVE, CINCINNATI, OH 45236 AND 425 WEST NATIONWIDE BOULEVARD, SUITE 300, COLUMBUS, OH 43215

Case No. 1:19MJ-496

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Brian Christ, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—four electronic devices and a large suitcase—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Transportation ("USDOT"), Office of Inspector General ("OIG"), in Columbus, Ohio. I have been employed as a USDOT-OIG Special Agent for approximately five years. I have successfully completed criminal investigator training at the Federal Law Enforcement Training Center in Glynco,

Georgia. As a Special Agent, I conduct criminal investigations of individuals and entities for possible violations of federal criminal laws, particularly those laws found in Title 18 and 49 of the U.S. Code that are relevant to the USDOT, Federal Motor Carrier Safety Administration ("FMCSA"). FMCSA responsibilities include monitoring and enforcing compliance with regulations governing safety and commerce related to interstate motor carriers, in particular Title 49, Code of Federal Regulations, Part 375, which governs the transportation of household goods by motor carriers. Further, I have specific experience and knowledge investigating the type of violations set forth below. I have participated in numerous search warrants at businesses and residences for documents, records, receipts, and computer-related equipment used to store information.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched are (1) a Galaxy Note 8 Cell Phone, currently stored at the Federal Bureau of Investigation ("FBI") offices in Cincinnati, Ohio; (2) a My Passport Portable Hard Drive, currently stored at FBI offices in Cincinnati, Ohio; (3) an LG Cell Phone, currently stored at FBI offices in Cincinnati, Ohio; (4) a Samsung Cell Phone, currently stored at FBI offices in Cincinnati, Ohio (collectively, hereinafter the "Devices"); and (5) a dark olive green and black large suitcase (Suitcase) with several fragile stickers and piece of papered taped to it with SERGEHI VERLAN's name on it, currently stored at FBI offices in Columbus, Ohio (hereinafter the "Suitcase"). The FBI offices in Cincinnati, OH are located at 2012 Ronald

Reagan Drive, Cincinnati, OH 45236 and the FBI office in Columbus, OH are located at 425 West Nationwide Boulevard, Suite 300, Columbus, OH 43215.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described and the search of the Suitcase and its contents, to include the forensic examination of any electronic devices, in Attachment B.

PROBABLE CAUSE

6. On July 25, 2018, a federal grand jury in the Southern District of Ohio returned an indictment charging SERGHEI VERLAN, as well as eleven of his co-conspirators, with participating in a RICO conspiracy through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(d). The indictment is attached and incorporated by reference.

7. As detailed in the indictment, the grand jury found probable cause that the defendants, along with corporate entities JBR Underground, LLC, United National Moving and Storage, National Relocation Solutions, Independent Van Lines, National Relocation Van Lines, US Relocation Systems, First National Moving and Storage, Public Moving and Storage, Public Moving Services, Smart Relocation Solutions, Presidential Moving Services, Unified Van Lines, and Flagship Van Lines (referred to collectively as "the affiliated companies"), and others known and unknown to the Grand Jury, constituted an "Enterprise" as defined in 18 U.S.C. § 1961(4), that is, a group of individuals and entities associated in fact that engaged in, and the activities of which affected, interstate and foreign commerce (referred to hereinafter as the "Moving Enterprise").

8. The grand jury found probable cause that the defendants violated § 1962(d) by knowingly and intentionally conspiring to conduct and participate in the conduct of the affairs of the Moving Enterprise through a pattern of racketeering activity, as defined in 18 U.S.C. §§ 1961(1) and (5), by conspiring to commit multiple acts of 18 U.S.C. § 1343 (relating to wire fraud); 18 U.S.C. § 659 (relating to the theft from interstate shipment); 18 U.S.C. § 1951(a) (relating to extortion); and 18 U.S.C. § 1028(a) (relating to fraud and related activity in connection with identification documents).

9. During the course of this investigation, I have obtained and executed search warrants of, among other things, Moving Enterprise offices, computers, and email accounts, including the personal Google email account of SERGHEI VERLAN. From the execution of those search warrants and my participation in this investigation, I have learned, among other things, the following:

a. Members of the Moving Enterprise, including VERLAN, relied upon email and electronic storage mediums to communicate and record the fraudulently inflated prices of the moves they conducted. For example, members of the Moving Enterprise emailed documents that showed customers were charged for more cubic feet than they actually used (e.g., documents would reference "real" or "actual" cubic feet).

b. Members of the Moving Enterprise, including VERLAN, used their cell phones to communicate about the operation of the Moving Enterprise, including the overcharging of customers and the filing of false documents to federal regulators.

c. Members of the Moving Enterprise also maintained paper records showing customers were charged for more cubic feet than they actually used.

d. VERLAN communicated regularly with employees through text message and email regarding the affairs of the Moving Enterprise, including communications relating to the actual cubic footage used in moves, which show that the Moving Enterprise was overcharging customers based on inflated cubic footage. I know based on my training and experience that individuals often retain text messages and emails on cell phones and other devices that store electronic information and/or can access the Internet.

e. VERLAN likely used his cell phone to save and/or take screenshots of text messages, documents, and videos related to the scheme. For example, (1) VERLAN made a video of himself explaining, in substance and in part, how to post fake reviews for the Moving Enterprise by creating Google accounts, posting the reviews, and then deleting the Google accounts; (2) VERLAN saved a screenshot of a text message from one of his co-conspirators, which read "ever[y]one ready for a new company," which, based on my knowledge and participation in this investigation, I believe this was a reference to the Moving Enterprise reincarnating as a new company through, in part, the submission of false documents to federal regulators; and (3) VERLAN took screenshots of bills of lading for customers of the Moving Enterprise, which indicated customers were charged for more cubic feet than they actually used.

10. The Devices and Suitcase are currently in the lawful possession of the FBI and USDOT-OIG. It came into FBI's and USDOT-OIG's possession in the following way: When I and other law enforcement began executing arrests of SERGHEI VERLAN's co-conspirators, VERLAN left the United States and fled to Panama. Based on my participation in this

investigation, I believe that VERLAN fled to Panama in order to avoid arrest in his case. On September 14, 2018, VERLAN was arrested on these charges by Panamanian authorities. At the time of his arrest, VERLAN had on his person the Devices and the Suitcase. Panamanian authorities seized the Devices and the Suitcase incident to arrest. On or about December 13, 2018, VERLAN was extradited from Panama to Cincinnati, Ohio. His extradition involved a stop in Florida. I and an agent with FBI personally accompanied VERLAN from Florida to Cincinnati, Ohio. At the time that the FBI agent and I took custody of VERLAN in Florida, another FBI Agent and USDOT-OIG Agent provided the Devices to us, who received them from the Panamanian authorities. The FBI agent and I took the Devices into custody and transported the Devices back to Ohio. The Suitcase was checked baggage in Panama and transported to the final destination in Cincinnati/Northern Kentucky International Airport (CVG)[1]. The FBI agent and I put the Devices and Suitcase into FBI custody soon after we arrived in Ohio. Therefore, while the USDOT-OIG and FBI might already have all necessary authority to examine the Devices and Suitcase, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

11. During the transport of SERGHEI VERLAN from Florida to Cincinnati, Ohio, VERLAN stated, in substance and in part, that the Devices were evidence that would help his case. As VERLAN fled, it is likely he may have stored other evidence and possibly devices of the scheme in the Suitcase. VERLAN stated that his suitcase contained everything that he

---

[1] The checked baggage did not make the connecting flight in Miami; therefore, it was transported to CVG on a later flight. On December 14, 2018, I picked up the suitcase from CVG and transported it to the FBI Office in Columbus, OH.

owned. [redacted] previously stated to agents during an interview following execution of a search warrant that VERLAN rarely worked in the office and that he ran the Moving Enterprise's operations from his personal phone and computer, which might be stored in the suitcase.

12. In addition, interviews following the Indictment indicate that VERLAN reached out to employees of the Moving Enterprise through phone calls, text messages, and direct messaging apps to discuss the allegations in the Indictment and alleged criminal activity committed by the Moving Enterprise. In addition, interviews indicate that he regularly used his computer and cell phone to operate the Moving Enterprise.[2]

13. The Devices are currently in storage at the FBI offices located at 2012 Ronald Reagan Drive, Cincinnati, OH 45236. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI. The Suitcase is currently in storage at the FBI offices located at 425 West Nationwide Boulevard, Suite 300, Columbus, OH 43215. In my training and experience, I know that the Suitcase has been stored in a manner in which its contents are, to the extent material to

---

[2] The interviews include statements from former employees whose identities are known to agents and who provided information that has been corroborated and deemed reliable and truthful. For example, [redacted], told agents [redacted] that VERLAN sent direct messages relating to the Moving Enterprise when he was in a Panamanian jail awaiting extradition in this case. In addition, [redacted] told agents [redacted] that VERLAN communicated regularly through email and direct messaging apps relating to particular moves.

this investigation, in substantially the same state as it was when the Suitcase first came into possession of the FBI and USDOT-OIG.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved

in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, PDAs, and electronic storage mediums. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

21. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices and Suitcase described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

22. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this

investigation will be searched at this time. In addition, sealing is necessary at this time to protect the identity of individuals who have provided information supporting probable cause until appropriate redactions can be made.

Respectfully submitted,

Brian J. Christ
Special Agent
U.S. DOT-OIG

Subscribed and sworn to before me

on July 2, 2019:

HON. KAREN L. LITKOVITZ
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched are (1) a Galaxy Note 8 Cell Phone, currently stored at the Federal Bureau of Investigation ("FBI") offices in Cincinnati, Ohio; (2) a My Passport Portable Hard Drive, currently stored at FBI offices in Cincinnati, Ohio; (3) an LG Cell Phone, currently stored at FBI offices in Cincinnati, Ohio; (4) a Samsung Cell Phone, currently stored at FBI offices in Cincinnati, Ohio (collectively, hereinafter the "Devices"); and (5) a large dark olive green and black suitcase, currently stored at FBI offices in Columbus, Ohio (hereinafter the "Suitcase"). The FBI offices in Cincinnati, OH are located at 2012 Ronald Reagan Drive, Cincinnati, OH 45236 and the FBI office in Columbus, OH are located at 425 West Nationwide Boulevard, Suite 300, Columbus, OH 43215.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B. This warrant authorizes the search of the Suitcase for the purpose of identifying information described in Attachment B.

ATTACHMENT B

1. All records and information relating to violations of 18 U.S.C. § 1962(d), those violations involving the financial or business affairs of JBR Underground, LLC, United National Moving and Storage, National Relocation Solutions, Independent Van Lines, National Relocation Van Lines, US Relocation Systems, First National Moving and Storage, Public Moving and Storage, Public Moving Services, Smart Relocation Solutions, Presidential Moving Services, Unified Van Lines, and Flagship Van Lines, and ANDREY SHUKLIN, SERGHEI VERLAN, PHYLLIS RICCI QUINCOCES, a/k/a "Faith Ashford," "Grace Rubestello," "Phyllis Ricci," EVGENIA KUKUY, a/k/a "Jenny K," "Evgenia Kukuv," VLADIMIR PESTEREANU, a/k/a "Vova," IEVGEN KAKIAKA, a/k/a "Eugene," AKHLIDDIN KALONOV, ROMAN IAKOVLEV, SANJAR FAYZIVEY, SERGEY BOCHAROV, JESSICA MARTIN, a/k/a "Emma Ricci," "Mary Austin," and SETH NEZAT, a/k/a "Andrew Johnson", "Andrew Butler," "Jason," "Kyle Walker," and others (referred to collectively as the "Moving Enterprise"), and occurring after April 2013, including:

a. Records and information showing ownership and control of the Moving Enterprise, and its affiliated companies, which may or may not have been mentioned above, including but not limited to the following:

(i) Corporate minutes, agreements, contracts, filings and correspondence reflecting, relating to, or concerning the Federal Motor Carrier Safety Administration (FMCSA), United States Department of Transportation (USDOT), various Secretary of State, to include but limited to Florida, North Carolina, Texas, Ohio, Illinois, Maryland and Connecticut;

(ii) Articles of personal property tending to establish the identity of persons in control of the premises, including but not limited to utility bills and receipts, rent receipts, cancelled mail envelopes, identification and/or travel documents and other items which establish personal identification;

b. Sales documents (including estimates, quotes and requests for quotes), bill of ladings, contracts, sales agreements, binding estimates, nonbinding estimates, revised estimates and other documents including correspondence, whether in draft or final form, concerning current or previously received requests or inquires for any customer of the Moving Enterprise and its affiliated companies, which may or may not have been mentioned above;

c. Records and information, including correspondence (recordings, records, facsimile, or e-mail) and files, relating to estimates, revised estimates, payment for services, charges for moves, cubic footage used in moves, storage of household goods, customer reviews, steps to evade federal regulators and law enforcement, and the transportation of household goods by the Moving Enterprise and its affiliated companies, which may or may not have been mentioned above;

d. Records and information relating to the identifies of employees, owners, and associates of the Moving Enterprise and its affiliated companies, which may or may not have been mentioned above;

e. Records and information relating to actual ownership of property in the custody and control of the Moving Enterprise and its affiliated companies, which may or may not have been mentioned above;

f. Payment information for household good moving services provided by the Moving Enterprise and its affiliated companies, which may or may not have been mentioned above, including financial records or documents, spreadsheets, records of payments, records of accounts payable and receivable, letters of credit, credit card invoices or authorization, bank checks, wire transfers;

g. Notes memorializing any conversation involving any estimates, revised estimates, transportation of household goods, the ownership of the Moving Enterprise and its affiliated companies, which may or may not have been mentioned above;

h. Tax returns, IRS filings, financial statements, any related work papers;

i. Records of personal or business activities relating to the operation or ownership of any computer hardware, software, storage media, or data (such as usernames, passwords telephone records, notes, books, diaries, and reference materials);

j. Records and information pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media;

k. All records and information related to personnel files containing, but not limited to, time cards, time sheets, payroll sheets, benefits paid, check stubs, jobs worked on, relating to current and former employees;

l. All records and information tending to show the identities of former employees, employees, associates or co-conspirators;

m. lists of customers and related identifying information;

n. all bank records, checks, credit card bills, account information, and other financial records;

o. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review any information removed from Devices in order to locate the things particularly described in this Warrant.